(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 102 49 842 A 1**

(51) Int. Cl.[7]: H 04 L 12/26

(21) Aktenzeichen: 102 49 842.3
(22) Anmeldetag: 25. 10. 2002
(43) Offenlegungstag: 28. 5. 2003

DE 102 49 842 A 1

(30) Unionspriorität:
001446 31. 10. 2001 US

(71) Anmelder:
Hewlett-Packard Co. (n.d.Ges.d.Staates Delaware), Palo Alto, Calif., US

(74) Vertreter:
Schoppe, Zimmermann, Stöckeler & Zinkler, 82049 Pullach

(72) Erfinder:
Tarquini, Richard Paul, Apex, N.C., US; Gales, George Simon, Plano, Tex., US

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Netz, Verfahren und computerlesbares Medium zum Verteilen von Sicherheitsaktualisierungen an ausgewählte Knoten auf einem Netz

(57) Ein Netz wird geschaffen, das ein Einbruchschutzsystem aufweist, das ein Netzmedium (200B), einen Verwaltungsknoten, der mit dem Netzmedium verbunden ist und eine Einbruchpräventationssystemverwaltungs-Anwendung betreibt, und eine Mehrzahl von Knoten, die mit dem Netzmedium verbunden sind und eine Instanz einer Einbruchschutzsystemanwendung betreiben, aufweist, wobei zumindest einer der Knoten eine Identifizierung aufweist, die demselben zugeordnet ist, basierend auf einer logischen Zuordnung, die einen oder mehrere der Mehrzahl von Knoten gruppiert, wobei jeder Knoten die Identifizierung teilt, die allgemein für zumindest eine Netzausbeutung anfällig ist.

DE 102 49 842 A 1

Beschreibung

[0001] Diese Erfindung bezieht sieh auf Netztechnologien und spezieller auf eine Technik zum Verteilen von Befehls- und Sicherheitsaktualisierungen an ausgewählte Knoten auf einem Netz.

[0002] Netzausbeutungs-Angriffswerkzeuge, wie DoS-Angriffsdienstprogramme (DoS = denial-of-service = Dienstverweigerung) werden technisch immer ausgereifter, und aufgrund der sich entwickelnden Technologien sind sie einfach auszuführen. Technisch relativ ungebildete Angreifer können Computersystembeeinträchtigungen arrangieren oder in dieselben involviert sein, die auf eine oder mehrere ins Ziel gefaßte Einrichtungen gerichtet sind. Ein Netzsystemangriff (der hierin auch als Eindringen bezeichnet wird) ist eine unautorisierte oder böswillige Verwendung eines Computers oder eines Computernetzes und kann Hunderte oder Tausende von ungeschützten oder anderweitig beeinträchtigte Internetknoten zusammen in einem koordinierten Angriff auf ein oder mehrere ausgewählte Ziele umfassen.

[0003] Netzangriffswerkzeuge basierend auf dem Client-/Servermodell sind zu einem bevorzugten Mechanismus zum Ausführen von Netzangriffen auf ins Ziel gefaßte Netze oder Vorrichtungen geworden. Hochkapazitätsmaschinen in Netzen, die über eine unzureichende Sicherheit verfügen, werden von Angreifern gerne genutzt, um verteilte Angriffe von denselben zu starten. Universitätsserver weisen typischerweise eine hohe Konnektivität und Kapazität, jedoch eine relativ mittelmäßige Sicherheit auf. Solche Netze haben auch häufig unerfahrene oder überarbeite Netzadministratoren, die die Netze für die Involvierung in Netzangriffe sogar noch anfälliger machen.

[0004] Netzausbeutungs-Angriffswerkzeuge, die feindliche Angriffsanwendungen wie DoS-Dienstprogramme aufweisen, die zum Übertragen von Daten über ein Netzmedium verantwortlich sind, weisen häufig eine unterscheidbare "Signatur" oder ein erkennbares Muster innerhalb der übertragenen Daten auf. Die Signatur kann eine erkennbare Sequenz von speziellen Paketen und/oder erkennbaren Daten aufweisen, die innerhalb von einem oder mehreren Paketen enthalten sind. Eine Signaturanalyse wird häufig durch ein Netz-IPS (IPS = intrusion prevention system = Einbruchpräventionssystem) ausgeführt und kann als ein Musterübereinstimmungsalgorithmus implementiert sein und kann andere Signaturerkennungsfähigkeiten sowie Anwendungsüberwachungs-Dienstprogramme einer höheren Ebene aufweisen. Ein einfacher Signaturanalysealgorithmus kann nach einer speziellen Zeichenfolge suehen, die als einer feindlichen Anordnung zugeordnet identifiziert worden ist. Sobald die Zeichenfolge innerhalb eines Netzdatenstroms identifiziert worden ist, können das eine oder die mehreren Pakete, die die Zeiehenfolge tragen, als "feindlich" oder ausbeutend identifiziert werden, und das IPS kann dann eine beliebige oder mehrere von einer Anzahl von Maßnahmen, wie Registrieren der Identifizierung des Rahmens, Ausführen einer Gegenmaßnahme oder Ausführen einer weiteren Datenarchivierungs- oder Schutzmaßnahme, ausführen.

[0005] Die IPS umfassen eine Technologie, die versueht, Ausbeutungen gegenüber einem Computersystem oder Netz von Computersystemen zu identifizieren. Zahlreiche Typen von IPS existieren und sind jeweils allgemein als entweder ein netzbasiertes, hostbasiertes oder knotenbasiertes IPS klassifiziert.

[0006] Die netzbasierten IPS-Vorrichtungen sind typiseherweise dedizierte (bzw. zweekgebundene) Systeme, die an strategisehen Stellen auf einem Netz plaziert sind, um Datenpakete zu untersuchen, um zu bestimmen, ob sie mit

bekannten Angriffssignaturen übereinstimmen. Um Pakete mit bekannten Angriffssignaturen zu vergleichen, nutzen die netzbasierten IPS-Vorrichtungen einen Mechanismus, der als eine passive Protokollanalyse bezeichnet wird, um den gesamten Verkehr auf einem Netz unauffällig zu überwaehen oder zu durehschnüffeln und um Ereignisse auf einer unteren Ebene, die von einem rohen Netzverkehr unterschieden werden können, zu erfassen. Die Netzausbeutungen können durch Identifizieren von Mustern oder andere beobachtbare Charakteristika von Netzrahmen erfaßt werden. Die netzbasierten IPS-Vorrichtungen untersuchen den Inhalt von Datenpaketen dureh syntaktisches Analysieren von Netzrahmen und Paketen und Analysieren individueller Pakete basierend auf den Protokollen, die auf dem Netz verwendet werden. Eine netzbasierte IPS-Vorrichtung überwacht auf unauffällige Weise den Netzverkehr, d. h. andere Netzknoten können sieh des Vorhandenseins der netzbasierten IPS-Vorrichtung nicht bewußt sein und tun dies auch häufig nicht. Eine passive Überwaehung wird normalerweise dureh eine netzbasierte IPS-Vorriehtung durch Implementieren eines "Wahllos-Modus"-Zugriffs von einer Netzschnittstellenvorrichtung ausgeführt. Eine Netzschnittstellenvorrichtung, die in dem wahllosen Modus arbeitet, kopiert Pakete direkt von dem Netzmedium, wie einem Koaxialkabel, einem 100baseT- oder anderem Übertragungsmedium, ungeachtet des Bestimmungsknotens, an den das Paket adressiert ist. Folglieh ist kein einfaehes Verfahren zum Übertragen von Daten über das Netzübertragungsmedium vorhanden, ohne daß die netzbasierte IPS-Vorrichtung dasselbe untersucht, und so kann die netzbasierte IPS-Vorriehtung den gesamten Netzverkehr, dem sie ausgesetzt ist, erfassen und analysieren. Nach der Identifizierung eines auffälligen Pakets, d. h. eines Pakets, das Attribute aufweist, die einer bekannten Angriffssignatur entsprechen, die auf ein Erscheinen durch die netzbasierte IPS-Vorrichtung überwacht wird, kann ein Alarm dadurch erzeugt werden und an ein Verwaltungsmodul des IPS übertragen werden, so daß ein Netzexperte Sieherheitsmaßnahmen umsetzen kann. Die netzbasierten IPS-Vorrichtungen haben den zusätzlichen Vorteil, daß sie in Echtzeit arbeiten und so einen Angriff, während dieser gesehieht, erfassen können. Außerdem ist eine netzbasierte IPS-Vorrichtung ideal zur Implementierung einer statusbasierten IPS-Sicherheitsmaßnahme, die eine Anhäufung und Speicherung von identifizierten auffälligen Paketen von Angriffen erfordert, die nieht "atomar" identifiziert werden können, d. h. durch ein einzelnes Netzpaket. Zum Beispiel sind TCP- (TCP = transmission eontrol protocol = Übertragungssteuerungsprotokoll) SYN- (SYN = synchronization = Synehronisierung) Flutattaeken nieht dureh ein einzelnes TCP-SYN-Paket identifizierbar, sondern werden allgemein vielmehr dureh ein Anhäufen eines Zählwerts von TCP-SYN-Paketen identifiziert, die eine vordefinierte Schwelle über einen definierten Zeitraum überschreiten. Eine netzbasierte IPS-Vorriehtung ist daher eine ideale Plattform zum Implementieren einer statusbasierten Signaturerfassung, weil die netzbasierte IPS-Vorrichtung alle diese TCP-SYN-Pakete sammeln kann, die sich über das lokale Netzmedium bewegen, und kann daher die Häufigkeit von solehen Ereignissen ordnungsgemäß archivieren und analysieren.

[0007] Die netzbasierten IPS-Vorrichtungen können jedoch häufig eine große Anzahl von "falsehen Positiven", d. h. unriehtigen Diagnosen eines Angriffs, erzeugen. Falsche Positivdiagnosen durch netzbasierte IPS-Vorrichtungen ergeben sich teilweise durch Fehler, die während einer passiven Analyse des Netzverkehrs erzeugt werden, die durch das IPS erfaßt werden, die in einer beliebigen Anzahl von netzunterstützten Protokollen verschlüsselt und forma-

tiert werden können. Ein inhaltsmäßiges Abtasten durch ein netzbasiertes IPS ist auf einer verschlüsselten Verknüpfung nicht möglich, obwohl die Signaturanalyse basierend auf Protokollanfangsblöcken ungeachtet dessen ausgeführt werden kann, ob die Verknüpfung verschlüsselt ist oder nicht. Zusätzlich sind die netzbasierten IPS-Vorrichtungen bei Hochgeschwindigkeitsnetzen häufig uneffektiv. Da Hochgeschwindigkeitsnetze immer üblicher werden, werden die software-basierten, netzbasierten IPS-Vorrichtungen, die versuchen, alle Pakete auf einer Verknüpfung zu durchschnüffeln, immer weniger zuverlässig. Am bedeutsamsten ist die Tatsache, daß die netzbasierten IPS-Vorrichtungen keine Angriffe verhindern können, es sei denn, sie sind in ein Brandmauerschutzsystem integriert und werden in Verbindung mit demselben betrieben.

[0008] Hostbasierte IPS erfassen Einbrüche durch Überwachen von Anwendungsschichtdaten. Hostbasierte IPS verwenden intelligente Agenten, um Computerprüfprotokolle auf auffällige Aktivitäten zu überprüfen und jede Veränderung in den Protokollen mit einer Bibliothek von Angriffssignaturen oder Benutzerprofilen zu vergleichen. Die hostbasierten IPS können auch Schlüsselsystemdateien und ausführbare Dateien auf unerwartete Veränderungen hin abrufen. Die hostbasierten IPS werden als solche bezeichnet, weil sich die IPS-Dienstprogramme auf dem System befinden, dem sie zugeordnet sind, um dasselbe zu schützen. Die hostbasierten IPS verwenden typischerweise Überwachungstechniken auf Anwendungsebene, die Anwendungsprotokolle untersuchen, die durch verschiedene Anwendungen unterhalten werden. Zum Beispiel kann ein hostbasiertes IPS eine Datenbankmaschine, die gescheiterte Zugriffsversuche und/oder Modifizierungen auf Systemkonfigurationen registriert, überwachen. Alarme können an einen Verwaltungsknoten nach der Identifizierung von Ereignissen geliefert werden, die von dem Datenbankprotokoll gelesen wurden, die als auffällig identifiziert worden sind. Hostbasierte IPS erzeugen allgemein sehr wenig falsche Positive. Hostbasierte IPS, wie Protokollwächter, sind jedoch allgemein auf ein Identifizieren von Einbrüchen beschränkt, die bereits stattgefunden haben, und sind auch auf Ereignisse beschränkt, die sich auf dem einzelnen Host ereignen. Weil sich die Protokollwächter auf ein Überwachen von Anwendungsprotokollen stützen, werden Schäden, die aus dem registrierten Angriff resultieren, allgemein bis zu dem Zeitpunkt, als der Angriff durch das IPS identifiziert worden ist, bereits stattgefunden haben. Einige hostbasierte IPS können einbruchspräventive Funktionen, wie "Einhaken" (Hooking) oder "Auffangen" (Intercepting) von Betriebssystems-Anwendungsprogrammierschnittstellen, ausführen, um die Ausführung von präventiven Operationen durch ein IPS basierend auf einer Anwendungsschichtaktivität, die einbruchsbezogen zu sein scheint, ausführen. Weil ein Einbruch, der in dieser Weise erfaßt wird, bereits ein beliebiges IPS auf unterer Ebene umgangen hat, stellt ein hostbasiertes IPS eine letzte Schicht der Verteidigung gegen eine Netzausbeutung dar. Die hostbasierten IPS sind jedoch zum Erfassen von Netzereignissen auf einer unteren Ebene, wie z. B. Protokollereignisse, nicht nützlich.

[0009] Die knotenbasierten IPS wenden die Einbruchserfassung und/oder Präventionstechnologie auf dem System an, das gesehützt wird. Ein Beispiel von knotenbasierten IPS-Technologien ist die Reihen-Einbruchserfassung (Inline-Einbruchserfassung). Ein knotenbasiertes IPS kann an jedem Knoten des Netzes, der geschützt werden soll, implementiert sein. Die Reihen-IPS (Inline-IPS) weisen Einbruchserfassungstechnologien auf, die in dem Protokollstapel des geschützten Netzknotens eingebettet sind. Weil das Reihen-IPS innerhalb des Protokollstapels eingebettet ist, bewegen sich sowohl eingehende als auch ausgehende Daten durch das Reihen-IPS und sind einer Überwachung durch dasselbe unterworfen. Ein Reihen-IPS überwindet viele der Schwächen, die netzbasierten Lösungen eigen sind. Wie vorstehend erwähnt ist, sind die netzbasierten Lösungen allgemein ineffektiv beim Überwachen von Hochgeschwindigkeitsnetzen aufgrund der Tatsache, daß die netzbasierten Lösungen versuchen, den gesamten Netzverkehr auf einer gegebenen Verknüpfung zu überwachen. Die Reihen-Einbruchspräventionssysteme überwachen jedoch nur den Verkehr, der an den Knoten gerichtet ist, auf dem das Reihen-IPS installiert ist. So können die Angriffspakete ein Reihen-IPS auf einer ins Ziel gefaßten Maschine nicht physisch umgehen, weil sich das Paket durch den Protokollstapel der ins Ziel gefaßten Vorrichtung bewegen muß. Eine beliebige Umgebung eines Reihen-IPS durch ein anderes Paket muß vollständig durch "logisches" Umgehen des IPS erfolgen, d. h. ein Angriffspaket, das ein Reihen-IPS vermeidet, muß dies in einer Weise tun, die bewirkt, daß das Reihen-IPS das Angriffspaket nicht oder nicht ordnungsgemäß identifiziert. Zusätzlich versehen die Reihen-IPS die Hostknoten mit Überwachungs- und Erfassungsfähigkeiten einer unteren Ebene, die jenen eines Netz-IPS ähneln, und können eine Protokollanalyse und Signaturübereinstimmung oder eine andere Überwachung oder Filterung des Hostverkehrs auf unterer Ebene liefern. Der wichtigste Vorteil, den die Reihen-IPS-Technologien bieten, ist, daß die Angriffe erfaßt werden, während sie geschehen. Während die hostbasierten IPS Angriffe dureh Überwaehen von Systemprotokollen bestimmen, involviert eine Reihen-Einbruehserfassung das Überwachen eines Netzverkehrs und das Isolieren jener Pakete, bei denen festgestellt wurde, daß sie Teil eines Angriffs gegen den Hostserver sind, und so ein Ermöglichen, daß das Reihen-IPS tatsächlich verhindert, daß der Angriff erfolgreich verläuft. Wenn bestimmt worden ist, daß ein Paket Teil eines Angriffs ist, kann die Reihen-IPS-Schicht das Paket aussortieren und somit verhindern, daß das Paket die obere Schicht des Protokollstapels erreicht, wo das Angriffspaket einen Schaden verursachen kann – ein Effekt, der im wesentlichen eine lokale Brandmauer für den Server erzeugt, der das Reihen-IPS hostet und dasselbe vor Bedrohungen schützt, die entweder aus einem externen Netz, wie dem Internet, oder aus dem Inneren des Netzes kommen. Ferner kann die Reihen-IPS-Schicht innerhalb des Protokollstapels bei einer Schicht eingebettet sein, wo die Pakete so verschlüsselt worden sind, daß das Reihen-IPS effektiv auf einem Netz mit verschlüsselten Verknüpfungen arbeitet. Zusätzlich kann das Reihen-IPS den ausgehenden Verkehr überwachen, weil sich sowohl der eingehende als auch der ausgehende Verkehr, der jeweils für einen Server bestimmt ist und von demselben entstammt, der das Reihen-IPS hostet, durch den Protokollstapel bewegen muß.

[0010] Obwohl die Vorteile der Reihen-IPS-Technologien zahlreich sind, bestehen bei der Implementierung eines solchen Systems einige Nachteile. Die Reihen-Einbruchserfassung ist allgemein prozessorintensiv und kann das Verhalten des Knotens, der das Erfassungsdienstprogramm hastet, beeinträchtigen. Zusätzlich können die Reihen-IPS zahlreiche falschpositive Angriffsdiagnosen erzeugen. Ferner können die Reihen-IPS ein systematisches Sondieren eines Netzes erfassen, wie ein solches, das durch Wiedererkennungsangriffs-Dienstprogramme ausgeführt wird, weil nur der Verkehr am lokalen Server, der das Reihen-IPS hostet, dadurch überwacht wird.

[0011] Jede der netzbasierten, hostbasierten und reihenbasierten IPS-Technologien weist jeweilige Vorteile, die vorstehend beschrieben sind, auf. Idealerweise umfaßt ein Ein-

bruchpräventionssystem alle zuvor erwähnten Einbruchserfassungsstrategien. Zusätzlich kann ein IPS einen oder mehrere Ereigniserzeugungsmechanismen aufweisen, die identifizierbare Ereignisse an eine oder mehrere Verwaltungseinrichtungen berichten. Ein Ereignis kann eine identifizierbare Serie von System- oder Netzbedingungen aufweisen oder sie kann eine einzelne identifizierte Bedingung aufweisen. Ein IPS kann auch einen Analysemechanismus- oder Modul aufweisen und kann Ereignisse analysieren, die durch den einen oder mehrere Ereigniserzeugnismechanismen erzeugt werden. Ein IPS kann ein Speicherungsmodul aufweisen, um Daten zu speichern, die den einbruchsbezogenen Ereignissen zugeordnet sind. Das IPS kann auch einen Gegenmaßnahmemechanismus aufweisen, um eine Maßnahme auszuführen, die eine erfaßte Ausbeutung vereiteln oder abwehren soll.

[0012] Die Steuerung und Verwaltung eines IPS, das zum Schützen eines großen Firmen- oder anderen Großnetzes konzipiert ist, erfordert Mechanismen zum Verteilen von Befehls- und Sicherheitsaktualisierungen von einem oder mehreren Verwaltungsknoten an versehiedene IPS-Server, die sich im Netz befinden. Da zum Beispiel neue Angriffe entwickelt und Signaturen und Gegenmaßnahmen dafür definiert sind, müssen die neu definierten Signaturen und Gegenmaßnahmen in die Knoten des Netzes, die durch den neuen Angriff ins Ziel gefaßt werden können, integriert werden. Tausende von Systemen können in einem Netz umfaßt und durch ein IPS geschützt sein. Die relativ häufige Einführung von neuen Angriffen erfordert Angriffsregeln, die zum Filtern eines Netzverkehrs, der routinemäßig aktualisiert werden soll, verwendet werden. Bekannte Systeme zur Verteilung von Befehls- und Sieherheitsaktualisierungen in einem IPS-gesehützten Netz umfassen ausgestrahlte (broadcast-mäßig) Aktualisierungen von einem zentralen Verwaltungsknoten und eine Installation von Sicherheitsaktualisierungen individuell an jedem Knoten, der IPS-Fähigkeiten aufweist. Das Ausstrahlen von Befehls- und Sicherheitsaktualisierungen erlaubt dem IPS-System netzweit von einer einzelnen Position aktualisiert zu werden, erfordert jedoch aber kostspielige hohe Bandbreitenverarbeitungsfähigkeiten am Verwaltungsknoten, der im Verhältnis zur Netzgröße skaliert. Das Aktualisieren von Angriffsregeln auf einer netzweiten Basis verbraucht wertvolle Netzbandbreite und erfordert eine entsprechend große Bandbreitenkapazität der Netzknoten. Die individuelle Installation von Sicherheitsaktualisierungen und eines jedes Knoten des Netzes ist aufgrund der erforderliehen Zeit und Arbeit, die zur vollen Aktualisierung des IPS erforderlich ist, unerwünseht.

[0013] Es ist eine Aufgabe der vorliegenden Erfindung, ein Netz, ein Verfahren und ein computerlesbares Medium zum Verteilen von Sicherheitsaktualisierungen an ausgewählte Knoten auf einem Netz zu schaffen, die mit geringeren Bandbreitenanforderungen auskommen.

[0014] Diese Aufgabe wird durch ein Netz gemäß Anspruch 1, ein Verfahren gemäß Anspruch 6 oder ein computerlesbares Medium gemäß Anspruch 10 gelöst.

[0015] Gemäß einem Ausführungsbeispiel der vorliegenden Erfindung wird ein Netz mit einem Einbruchsschutzsystem gesebaffen, das ein Netzmedium, einen Verwaltungsknoten, der mit dem Netzmedium verbunden ist und eine Einbruchpräventionssystem-Verwaltungsanwendung betreibt, aufweist, und eine Mehrzahl von Knoten, die mit dem Netzmedium verbunden sind und eine Instanz (bzw. Exemplar) einer Einbruchsschutzsystem-Anwendung betreiben, aufweist, wobei zumindest einer der Knoten eine Identifizierung aufweist, die demselben zugeordnet ist, basierend auf einer logischen Zuordnung, die einen oder mehrere der Mehrzahl von Knoten gruppiert, wobei jeder Knoten die Identifizierung teilt, die allgemein für zumindest eine Netzausbeutung anfällig ist.

[0016] Gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung wird ein Verfahren zum Übertragen einer Befehls- und Sicherheitsaktualisierungsnachricht an einen Teilsatz von Knoten einer Mehrzahl von Netzknoten geschaffen, das ein Erzeugen einer Aktualisierungsnachricht durch einen Verwaltungsknoten des Netzes, ein Adressieren der Aktualisierungsnachricht an eine Netzadresse, die durch den Teilsatz von Knoten geteilt wird, ein Übertragen der Aktualisierungsnachricht und ein Empfangen und Verarbeiten der Aktualisierungsnachricht durch den Teilsatz von Knoten aufweist.

[0017] Gemäß einem weiteren Ausführungsbeispiel der vorliegenden Erfindung wird ein computerlesbares Medium geschaffen, auf dem ein Satz von Instruktionen, die ausgeführt werden sollen, gespeichert ist, wobei der Satz von Instruktionen, wenn dieselben dureh einen Prozessor ausgeführt werden, bewirken, daß der Prozessor ein Computerverfahren zum Erzeugen, durch den Computer, einer Nachricht, die an einen Teilsatz von Knoten auf einem Netz adressiert ist, zum Übertragen der Nachricht auf einem Netzmedium des Netzes an den Teilsatz von Knoten, zum Empfangen der Nachricht durch einen Router, der am Netzmedium endet, und zum Weiterleiten, dureh den Router, der Nachricht an beliebige Knoten, die in dem Teilsatz von Knoten auf einem zweiten Netzmedium enthalten sind, das durch den Router beendet wird, ausführt.

[0018] Bevorzugte Ausführungsbeispiele der vorliegenden Erfindung werden nachfolgend Bezug nehmend auf die beiliegenden Zeichnungen näher erläutert. Es zeigen:

[0019] **Fig. 1** eine exemplarische Anordnung zum Ausführen einer Computersystembeeinträchtigung gemäß dem Stand der Technik;

[0020] **Fig. 2** ein umfassendes Einbruchspräventionssystem, das netzbasierte und hybrid-hostbasierte und knotenbasierte Einbrucherfassungstechnologien gemäß einem Ausführungsbeispiel der Erfindung nutzt;

[0021] **Fig. 3** einen exemplarischen Netzprotokollstapel gemäß dem Stand der Technik;

[0022] **Fig. 4** einen Netzknoten, der ein Beispiel (Instanz) einer Einbruchsschutzsystem-Anwendung gemäß einem Ausführungsbeispiel der vorliegenden Erfindung betreiben kann;

[0023] **Fig. 5** einen exemplarischen Netzknoten, der als ein Verwaltungsknoten innerhalb eines Netzes arbeiten kann, das dureh das Einbruehsschutzsystem gemäß einem Ausführungsbeispiel der vorliegenden Erfindung geschützt ist;

[0024] **Fig. 6** eine vereinfaehte Darstellung eines Netzes, das ein Unternehmens-Einbruehpräventionssystem gemäß einem Ausführungsbeispiel der vorliegenden Erfindung, die auf demselben eingesetzt werden kann, aufweist; und

[0025] **Fig. 7** eine logische Gruppierung von Knoten, die in einem Netz angeordnet sind, die einen Gruppensenden (Multicast) von Befehls- und Sicherheitsaktualisierungen von einem Verwaltungsknoten gemäß einem Ausführungsbeispiel der vorliegenden Erfindung erleichtert.

[0026] Das bevorzugte Ausführungsbeispiel der vorliegenden Erfindung und seine Vorteile werden unter Bezugnahme auf **Fig. 1** bis 7 der Zeichnungen, wo identische Bezugszeiehen für identische und entsprechende Teile der verschiedenen Zeichnungen verwendet werden, am besten verständlich.

[0027] In **Fig. 1** ist eine exemplarische Anordnung zum Ausführen einer Computersystembeeinträchtigung dargestellt, wobei das dargestellte Beispiel eine vereinfachte Anordnung des verteilten Einbruchsnetzes **40** zeigt, die typisch

für verteilte Systemangriffe ist, die auf eine Zielmaschine **30** gerichtet sind. Eine Angriffsmaschine **10** kann eine Ausführung eines verteilten Angriffs durch eine beliebige Anzahl von Angreiferangriffsagenten **20A–20N** durch eine von zahlreichen Techniken, wie einer Fernsteuerung durch die IRC-Roboteranwendungen, anweisen. Die Angriffsagenten **20A–20N**, die auch als "Zombies" und "Angriffsagenten" bezeichnet werden, sind allgemein Computer, die zur öffentlichen Nutzung verfügbar sind oder die so beeinträchtigt worden sind, daß ein verteilter Angriff im Anschluß an einen Befehl einer Angriffsmaschine **10** gestartet werden kann. Zahlreiche Typen von verteilten Angriffen können gegen eine Zielmaschine **30** gestartet werden. Die Zielmaschine **30** kann einen umfassenden Schaden durch gleichzeitige Angriffe durch die Angriffsagenten **20A–20N** erleiden, und die Angriffsagenten **20A–20N** können durch die Client-Angriffsanwendung ebenso beschädigt werden. Ein verteiltes Einbruchsnetz kann eine zusätzliche Schicht von Maschinen aufweisen, die in einen Angriff zwischen der Angriffsmaschine **10** und den Angriffsagenten **20A–20N** involviert sind. Diese Zwischenmaschinen werden allgemein als "Handhabungseinrichtungen" ("Handler") bezeichnet und jede Handhabungseinrichtung kann einen oder mehrere Angriffsagenten **20A–20N** steuern. Die Anordnung, die zum Ausführen einer Computersystembeeinträchtigung gezeigt ist, ist nur illustrativ und kann zahlreiche Anordnungen beeinträchtigen, die so einfach sind wie eine einzelne Angriffsmaschine **10**, die eine Zielmaschine **30** durch z. B. Senden eines bösartigen Sondierungspakets oder anderer Daten, die die Zielmaschine **30** beeinträchtigen sollen, angreift. Die Zielmaschine kann mit einem größeren Netz verbunden sein und ist dies auch häufig, und ein Angriff auf dieselbe durch die Angriffsmasehine **10** kann einen Schaden an einer großen Ansammlung von Computersystemen bewirken, die sich häufig innerhalb des Netzes befinden.

[0028] In **Fig. 2** ist ein umfassendes Einbruchspräventionssystem dargestellt, das netzbasierte und hybridhostbasierte/knotenbasierte Einbruchserfassungstechnologien gemäß einem Ausführungsbeispiel der Erfindung nutzt. Ein oder mehrere Netze **100** können mit dem Internet **50** über einen Router **45** oder eine andere Vorrichtung sehnittstellenmäßig verbunden sein. Bei dem veranschaulichenden Beispiel weist das Netz **100** zwei Ethernet-Netze **55** und **56** auf. Das Ethernet-Netz **55** weist einen Webinhaltsserver **270A** und einen Dateitransport-Protokollinhaltsserver **270B** auf. Das Ethernet-Netz **56** weist einen Domain-Namenserver **270C**, einen Mail-Server **270D**, einen Datenbank-Server **270E** und einen Dateiserver **270F** auf. Ein Brandmauer-/Proxy-Router **60**, der zwischen den Ethernets **55** und **56** angeordnet ist, liefert für die verschiedenen Systeme des Netzes **56** eine Sicherheits- und Adreßauflösung. Eine netzbasierte IPS-Vorrichtung **80** und **81** ist jeweils auf beiden Seiten des Brandmauer-/Proxy-Routers **60** implementiert, um die Überwachung von versuchten Angriffen auf ein oder mehrere Elemente der Ethernet-Netze **55** und **56** zu erleichtern und um eine Aufzeichnung von erfolgreichen Angriffen zu erleichtern, die den Brandmauer-/Proxy-Router **60** erfolgreich durchdringen. Die netzbasierten IPS-Vorriehtungen **80** und **81** können jeweils eine Datenbank **80A** und **81A** der bekannten Angriffssignaturen oder Regeln aufweisen (oder alternativ mit derselben verbunden sein), mit denen die Netzrahmen, die dadurch erfaßt wurden, verglichen werden können. Alternativ kann eine einzelne Datenbank (nicht gezeigt) innerhalb eines Netzes **100** zentral angeordnet sein, und netzbasierte IPS-Vorrichtungen **80** und **81** können auf dieselbe zugreifen. Dementsprechend kann die netzbasierte IPS-Vorrichtung **80** alle Pakete, die vom Internet **50** in das Netz **100** eingehen und am Ethernet-Netz **55** ankommen, überwaehen. Desgleichen kann eine netzbasierte IPS-Vorrichtung **81** alle Pakete, die durch den Brandmauer-/Proxy-Router **60** zur Auslieferung an das Ethernet-Netz **56** passiert werden, überwachen und vergleichen. Ein IPS-Verwaltungsknoten **85** kann auch Teil des Netzes **100** sein, um die Konfiguration und Verwaltung der IPS-Komponenten im Netz **100** zu erleichtern.

[0029] Angesichts der vorstehend angemerkten Unzulänglichkeiten der netzbasierten Einbruchspräventionssysteme ist vorzugsweise ein hybrid-hostbasiertes und knotenbasiertes Einbruchspräventionssystem innerhalb eines jeden der verschiedenen Knoten, wie den Servern **270A–270N** (die hierin auch als "Knoten" bezeichnet werden), des Ethernet-Netzes **55** und **56** im gesicherten Netz **100** implementiert. Der Verwaltungsknoten **85** kann Alarmmitteilungen von den jeweiligen Knoten innerhalb des Netzes **100** nach der Erfassung eines Einbruchsereignisses durch eine beliebige der netzbasierten IPS-Vorriehtungen **80** und **81** sowie einen beliebigen der Knoten des Netzes **100**, auf dem ein hybrid-agentenbasiertes und knotenbasiertes IPS implementiert ist, empfangen. Zusätzlich kann jeder Knoten **270A–270F** ein lokales Dateisystem zum Arehivieren von einbruchsbezogenen Ereignissen, zum Erzeugen von einbruchsbezogenen Meldungen und zum Speichern von Signaturdateien, im Vergleich zu denen die lokalen Netzrahmen und/oder Pakete untersucht werden, nutzen.

[0030] Vorzugsweise sind die netzbasierten IPS-Vorrichtungen **80** und **81** dedizierte Entitäten zum Überwachen des Netzverkehrs auf den zugeordneten Ethernets **55** und **56** des Netzes **100**. Um die Einbruchserfassung bei Hochgeschwindigkeitsnetzen zu erleichtern, weisen die netzbasierten IPS-Vorrichtungen **80** und **81** vorzugsweise einen großen Erfassungs-RAM zum Erfassen von Paketen auf, da diese auf den jeweiligen Ethernet-Netzen **55** und **56** ankommen. Zusätzlich wird bevorzugt, daß die netzbasierten IPS-Vorrichtungen **80** und **81** jeweils hardwarebasierte Filter zum Filtern des Netzverkehrs aufweisen, obwohl ein IPS-Filtern durch die netzbasierten IPS-Vorrichtungen **80** und **81** in einer Software implementiert sein kann. Außerdem können die netzbasierten IPS-Vorrichtungen **80** und **81** z. B. durch Anforderung des IPS-Verwaltungsknotens **85** konfiguriert sein, um eine oder mehrere spezifische Vorrichtungen und nicht alle Vorriehtungen auf einem gemeinsamen Netz zu überwaehen. Zum Beispiel kann eine netzbasierten IPS-Vorrichtung **80** angewiesen werden, nur den Netzdatenverkehr zu überwachen, der an den Webserver **270A** adressiert ist.

[0031] Die hybrid-hostbasierten/knoten-basierten Einbruchspräventionssystemtechnologien können auf allen Knoten **270A–270N** auf den Ethernet-Netzen **55** und **56** implementiert sein, die durch einen Netzangriff ins Ziel gefaßt werden können. Allgemein besteht jeder Knoten aus einem umprogrammierbaren Computer mit einer CPU (CPU = central processing unit zentrale Verarbeitungseinheit), einem Speichermodul, das betreibbar ist, um einen maschinenlesbaren Code zu speiehern, der durch die CPU wiedergewinnbar und ausführbar ist, und kann ferner verschiedene Peripherievorrichtungen, wie einen Anzeigemonitor, eine Tastatur, eine Maus und eine andere Vorriehtung, die mit demselben verbunden sind, aufweisen. Ein Speicherungsmedium, wie eine Magnetplatte, eine optische Platte oder eine andere Komponente, die zum Speichern von Daten betreibbar ist, kann mit dem Speichermodul verbunden sein und dadurch zugreifbar sein und kann eine oder mehrere Datenbanken zum Archivieren von lokalen Einbruchsereignissen und Einbruehsereignisberiehten liefern. Ein Betriebssystem kann in das Speichermodul, z. B. naeh dem Booten des jeweiligen Knotens, geladen werden und eine Instanz eines Protokollstapels sowie verschiedene Softwaremodule der

unteren Ebene aufweisen, die für Aufgaben, wie ein schnittstellenmäßiges Verbinden mit einer Peripheriehardware, ein Planen von Aufgaben, eine Zuweisung der Speicherung sowie anderer Systemaufgaben, erforderlich sind. Jeder Knoten, der durch das hybrid-hostbasierte und knotenbasierte IPS der vorliegenden Erfindung geschützt ist, weist dementsprechend eine IPS-Softwareanwendung auf, die innerhalb des Knotens beibehalten wird, wie in einer magnetischen Festplatte, die durch das Betriebssystem wiedergewinnbar und dureh die zentrale Verarbeitungseinheit ausführbar ist. Zusätzlich weist jeder Knoten, der eine Instanz der IPS-Vorrichtung ausführt, eine lokale Datenbank auf, von der aus Signaturbesehreibungen von dokumentierten Angriffen vom Speicher geholt und mit einem Paket oder Rahmen von Daten verglichen werden können, um eine Entsprechung zwischen denselben zu erfassen. Die Erfassung einer Entsprechung zwischen einem Paket oder Rahmen an einem IDS-Server kann zur Ausführung von einer beliebigen oder mehreren von verschiedenen Sicherheitsprozeduren führen.

[0032] Das unter Bezugnahme auf **Fig. 2** besehriebene IPS kann auf einer beliebigen Anzahl von Plattformen implementiert sein. Jede hybrid-hostbasierte/knoten-basierte Instanz der IPS-Vorrichtung, die hierin besehrieben ist, ist vorzugsweise auf einem Netzknoten, wie einem Webserver **270A**, implementiert, der unter Steuerung eines Betriebssystems, wie Windows NT 4.0 betrieben wird, das in einem Hauptspeicher gespeichert ist und auf einer zentralen Verarbeitungseinheit arbeitet, und versucht, Angriffe, die auf den Hostknoten gerichtet sind, zu erfassen. Das spezielle Netz **100**, das in **Fig. 2** dargestellt ist, ist nur exemplariseh und kann eine beliebige Anzahl von Netzknoten, wie Netzserver oder Computer aufweisen. Firmen- und/oder andere Großnetze können typischerweise zahlreiche individuelle Systeme aufweisen, die ähnliche Dienste anbieten. Zum Beispiel kann ein Firmennetz Hunderte von einzelnen Webservern, Mailservern, FTP-Servern und anderen Systemen aufweisen, die gemeinsame Datendienste anbieten.

[0033] Jedes Betriebssystem eines Knotens, der eine Instanz einer IPS-Vorrichtung umfaßt, weist zusätzlich einen Netzprotokollstapel **90** auf, der in **Fig. 3** dargestellt ist, der den Eingangspunkt für Rahmen definiert, die dureh einen ins Ziel gefaßten Knoten aus dem Netz, z. B. dem Internet oder Intranet, empfangen werden. Der dargestellte Netzstapel **90** stellt den hinreichend bekannten Windows-NT-(TM)-Systemnetzprotokollstapel dar und ist so ausgewählt worden, um die Erörterung und das Verständnis der Erfindung zu erleichtern. Es wird jedoch darauf hingewiesen, daß die Erfindung nicht auf eine spezifisehe Implementierung des dargestellten Netzstapels **90** beschränkt ist, sondern vielmehr auf den Stapel **90**, der beschrieben ist, um das Verständnis der Erfindung zu erleichtern. Der Netzstapel **90** weist eine TDI (TDI = transport driver interfaee = Transporttreiberschnittstelle) **125**, einen Transporttreiber **130**, einen Protokolltreiber **135** und einen MAC-Treiber (MAC = media access eontrol = Medienzugriffssteuerung) **145** auf, der mit dem physischen Medium **101** schnittstellenmäßig verbunden ist. Die Transporttreiberschnittstelle **125** funktioniert, um den Transporttreiber **130** mit den Dateisystemtreibern einer höheren Ebene schnittstellenmäßig zu verbinden. Dementsprechend ermöglicht die TDI **125** den Betriebssystemtreibern, wie den Netzumleitern, eine Sitzung zu aktivieren oder an den entsprechenden Protokolltreiber **135** zu binden. Folglieh kann ein Umleiter auf das entspreehende Protokoll, z. B. ein UDP, TCP, NetBEUI oder anderes Netz- oder Transportschichtprotokoll, zugreifen, wodurch der Umleiter protokollunabhängig gemaeht wird. Der Protokolltreiber **135** erzeugt Datenpakete, die vom Computer, der den Netzprotokollstapel **90** hostet, auf einen anderen Computer oder eine andere Vorrichtung auf dem Netz oder einem anderen Netz über das physisehe Medium **101** gesendet werden. Typische Protokolle, die durch einen NT-Netzprotokollstapel unterstützt werden, weisen NetBEUI, TCP/IP, NWLink, DLC (DLC = data link eontrol = Datenverknüpfungssteuerung) und AppleTalk auf, obwohl andere Transport- und/oder Netzprotokolle umfaßt sein können. Ein MAC-Treiber **145**, z. B. ein Ethernet-Treiber, ein Token-Ring-Treiber oder ein anderer Netzbetriebstreiber, ermöglicht ein entsprechendes Formatieren und schnittstellenmäßiges Verbinden mit dem physischen Medium **101**, wie einem Koaxialkabel oder einem anderen Übertragungsmedium.

[0034] Die Fähigkeiten des hostbasierten IPS weisen die Anwendungsüberwachung von Dateisystemereignissen; einem Registrierzugriff; von erfolgreichen Sicherheitsereignissen; gescheiterten Sicherheitsereignissen und einer auffälligen Prozeßüberwachung auf. Bei Netzzugriffsanwendungen, wie einem Mierosoft-IIS- und SQL-Server, können Prozesse, die auf dieselben bezogen sind, ebenfalls überwacht werden.

[0035] Einbrüche können auf einem speziellen IPS-Host dureh Implementieren von knotenbasierten Reihenüberwachungstechnologien (Inline-Überwachungstechnologien) verhindert werden. Das Reihen-IPS (Inline-IPS) ist vorzugsweise als Teil eines hybrid-hostbasierten/knoten-basierten IPS umfaßt, obwohl es unabhängig von einem beliebigen hostbasierten IPS-System implementiert sein kann. Das Reihen-IPS analysiert die Pakete, die am Hostknoten empfangen werden, und führt eine Signaturanalyse derselben gegenüber einer Datenbank von bekannten Signaturen durch ein Netzschichtfiltern aus.

[0036] In **Fig. 4** ist ein Netzknoten **270** dargestellt, der eine Instanz einer IPS-Vorrichtung **91** betreiben kann und so als ein IPS-Server operieren kann. Die IPS-Vorrichtung **91** kann als eine dreischichtige IPS, wie in einer ebenfalls anhängigen US-Anmeldung mit dem Titel "Method, Computer Readable Medium, and Node for a Three-Layered Intrusion Prevention System for Detecting Network Exploits", die gleichzeitig mit der Anmeldung, deren Priorität hierin beansprueht wird, eingereicht wurde und auf die gleiche Inhaberin übertragen wurde, beschrieben ist, implementiert sein und kann eine Serveranwendung und/oder eine Client-Anwendung aufweisen. Der Netzknoten **270** weist allgemein eine CPU **272** und ein Speichermodul **274** auf, das betreibbar ist, um einen maschinenlesbaren Code zu speichern, der durch die CPU **272** über einen Bus (nicht gezeigt) wiedergewinnbar und ausführbar ist. Ein Speieherungsmedium **276**, wie eine Magnetplatte, eine optische Platte oder eine andere Komponente, die betreibbar ist, um Daten zu speichern, kann mit einem Speiehermodul **274** verbunden sein und dadureh dureh den Bus ebenso zugreifbar sein. Ein Betriebssystem **275** kann in das Speichermodul **274**, z. B. nach dem Booten des Knotens **270**, geladen werden und eine Instanz des Protokollstapels **90** aufweisen und bewirken, daß eine Einbruchspräventionssystemanwendung **91** vom Speicherungsmedium **276** geladen wird. Eine oder mehrere Netzausbeutungsregeln, eine exemplarisehe Form, die in der ebenfalls anhängigen Anmeldung mit dem Titel "Method, Node and Computer Readable Medium for Identifying Data in a Network Exploit", die gleichzeitig hiermit eingereicht wird, besehrieben ist, kann zu maschinenlesbaren Signaturen kompiliert und innerhalb einer Datenbank **277** gespeichert sein, die in das Speichermodul **274** ladbar ist, und kann durch die IPS-Vorrichtung **91** zum Erleichtern einer Analyse von Netzrahmen und/oder Paketen wiedergewonnen werden.

[0037] In **Fig. 5** ist ein exemplarischer Netzknoten darge-

stellt, der als ein Verwaltungsknoten **85** des IPS eines Netzes **100** arbeiten kann. Der Verwaltungsknoten **85** weist allgemein eine zentrale Verarbeitungseinheit **272** und ein Speichermodul **274** auf, die betreibbar sind, um einen maschinenlesbaren Code zu speichern, der durch die CPU **272** über einen Bus (nicht gezeigt) wiedergewinnbar und ausführbar ist. Ein Speicherungsmedium **276**, wie eine Magnetplatte, eine optische Platte oder eine andere Komponente, die betreibbar ist, um Daten zu speichern, kann mit dem Speichermodul **274** verbunden sein und ist dadurch auch durch den Bus zugreifbar. Ein Betriebssystem **275** kann in das Speichermodul **274**, z. B. nach dem Booten des Knotens **85**, geladen werden und eine Instanz des Protokollstapels **90** aufweisen. Das Betriebssystem **275** ist betreibbar, um eine IPS-Verwaltungsanwendung **279** vom Speicherungsmedium **276** zu holen und die Verwaltungsanwendung **279** in das Speichermodul **274** zu laden, wo sie durch die CPU **272** ausgeführt wird. Der Knoten **85** weist vorzugsweise eine Eingabevorriehtung **281**, wie eine Tastatur, und eine Ausgabevorrichtung **282**, wie einen Monitor, der mit demselben verbunden ist, auf.

[0038] Ein Operator des Verwaltungsknotens **85** kann eine oder mehrere Textdateien **277A–277N** über die Eingabevorrichtung **281** eingeben. Jede Textdatei **277A–277N** kann eine netzbasierte Ausbeutung definieren und eine logische Beschreibung einer Angriffssignatur sowie IPS-Anweisungen zum Ausführen nach einer IPS-Auswertung eines einbruchsbezogenen Ereignisses, das der beschriebenen Angriffssignatur zugeordnet ist, aufweisen. Jede Textdatei **277A–277N** kann in einer Datenbank **278A** auf einem Speicherungsmedium **276** gespeichert sein und durch einen Kompilierer **280** in eine jeweilige maschinenlesbare Signaturdatei **281A–281N** kompiliert werden, die in einer Datenbank **278B** gespeichert ist. Jede der maschinenlesbaren Signaturdateien **281A–281N** weist einen binären logischen Stellvertreter der Angriffssignatur, die in der jeweiligen zugeordneten Textdatei **277A–277N** beschrieben ist, auf. Ein Operator des Verwaltungsknotens **85** kann den Verwaltungsknoten **85** durch Interaktion mit einer Client-Anwendung der IPS-Vorrichtung **279** über eine Eingabevorriehtung **281** periodisch anweisen, eine oder mehrere maschinenlesbare Signaturdateien (die hierin auch allgemein als "Signaturdateien" bezeichnet werden), die in der Datenbank **278B** gespeichert sind, an einen Knoten oder eine Mehrzahl von Knoten im Netz **100** zu übertragen. Alternativ können die Signaturdateien **281A–281N** in einem computerlesbaren Medium, wie einer Kompaktdisk, einer Magnet-Diskette oder einer anderen tragbaren Speicherungsvorrichtung, gespeichert sein und auf dem Knoten **270** des Netzes **100** installiert sein. Die Anwendung **279** ist vorzugsweise betreibbar, um alle solchen Signaturdateien **281A–281N** oder einen oder mehrere Teilsätze derselben an einen Knoten oder eine Mehrzahl von Knoten im Netz **100** zu übertragen. Vorzugsweise stellt die IPS-Vorrichtung **279** eine graphische Benutzerschnittstelle auf der Ausgabevorrichtung **282** zum Erleichtern der Eingabe von Befehlen in dieselbe durch einen Operator des Knotens **85** bereit.

[0039] Während neue Angriffe entwickelt und Signaturen und Gegenmaßnahmen dafür definiert werden, müssen die neu definierten Signaturen und Gegenmaßnahmen in das IPS, das innerhalb der geschützten Knoten des Netzes implementiert ist, die durch den neuen Angriff ins Ziel gefaßt werden können, und/oder in die netzbasierte IPS-Vorrichtungen integriert werden, die zugeordnet sein können, um das Netz zu schützen. Folglich erfordert die Steuerung und Verwaltung eines IPS, das zum Schützen eines großen Firmen- oder anderen Großnetzes konzipiert ist, Mechanismen zum Verteilen von Befehls- und Sieherheitsaktualisierungen von einem oder mehreren Verwaltungsknoten an verschiedene IPS-Server, die im Netz positioniert sind.

[0040] Die vorliegende Erfindung schafft einen Mechanismus zum Reduzieren der erforderlichen Bandbreitenkapazität einer Verwaltungskonsole und erleichtert eine Reduktion der Netzbandbreite, die verbraucht wird, wenn die Befehls- und Sicherheitsaktualisierungen von einer Verwaltungskonsole innerhalb eines Netzes verteilt werden, indem einem Teilsatz von ausgewählten Knoten ermöglicht wird, von einer zentralen Verwaltungskonsole in einer Weise aktualisiert zu werden, die unnotwendige Aktualisierungen umgeht, die auf den Knoten ausgeführt werden, die durch eine Sicherheitsaktualisierung nachteilig beeinträchtigt werden können.

[0041] Unter Bezugnahme auf **Fig. 6** ist ein vereinfachtes Netz **200** dargestellt, das ein Unternehmens-Einbruchpräventionssystem aufweisen kann, das vorzugsweise netzbasierte und hybridhostbasierte und knotenbasierte Einbrucherfassungstechnologien gemäß einem Ausführungsbeispiel der Erfindung vorzugsweise verwendet. Ein geschütztes Netz **200** kann ein oder mehrere Teilnetze wie die Ethernet-Netze **200A–200N** umfassen, die mit jeweiligen Routern **106A–106M** schnittstellenmäßig verbunden sind. Das Netz **200** kann mit dem Internet **50** über einen Router **40** schnittstellenmäßig verbunden sein. Das beispielhafte Ethernet **200A** umfaßt eine Mehrzahl von Web-Servern **201A–201L**, eine Mehrzahl von FTP-Servern **203A–203M** und eine Mehrzahl von Datenbankservern **207A-207N**. Eine netzbasierte IPS-Vorriehtung **180** ist vorzugsweise mit dem Ethernet **200A** über eine Netzschnittstellenkarte (nicht gezeigt) verbunden, die in einem "wahllosen Modus" arbeitet und betreibbar ist, um auffällige Netzrahmen, die auf dem Ethernet **200A** empfangen werden, zu scannen und zu identifizieren. Ein Brandmauer-/Proxyrouter **160A** kann das Ethernet **200A** mit dem Ethernet **200B** schnittstellenmäßig verbinden und erleichtert ein Weiterleiten von Paketen zwischen denselben und liefert Sicherheitsmaßnahmen und/oder Proxy-Dienste, um den Zugriff auf das Internet **50** für die Knoten auf den Ethernet-Netzen **200B-200N** zu erleichtern. Das beispielhafte Ethernet **200B** umfaßt einen Domain-Namenserver **170**, eine Mehrzahl von Dateiservern **205A–205Q**, eine Mehrzahl von Datenbankservern **208A–208P** und eine Mehrzahl von Mailservern **210A–210R**. Das Ethernet **200B** kann eine netzbasierte IPS-Vorrichtung **181** aufweisen, die betreibbar ist, um auffällige Netzrahmen, die über das Ethernet **200B** übertragen werden, zu überwachen und zu identifizieren. Eine Mehrzahl von anderen Netzen **200C–200M** (nicht gezeigt) kann mit dem Netz **200** verbunden sein oder in demselben umfaßt sein. Ein exemplarisches finales Ethernet **200N** kann mit anderen Ethernet-Netzen **200A–200M** über einen Brandmauer-/Proxyrouter **160M** schnittstellenmäßig verbunden sein. Das beispielhafte Ethernet **200N** umfaßt eine Mehrzahl von Webservern **202A–202T**, eine Mehrzahl von FTP-Servern **204A–204U**, eine Mehrzahl von Dateiservern **206A–206V**, eine Mehrzahl von Datenbankservern **209A–209W** und eine Mehrzahl von Mailservern **211A–211X** sowie eine netzbasierte IPS-Vorriehtung **182**, die betreibbar ist, um auffällige Netzrahmen, die über das Ethernet **200N** übertragen werden, zu überwachen und zu identifizieren. Zusätzlich sind ein oder mehrere IPS-Verwaltungsknoten **85** mit dem Netz **200** verbunden und können Alarmnachrichten von den jeweiligen Knoten innerhalb des Netzes **200** nach einer Erfassung eines Einbruchsereignisses empfangen sowie eine Verteilung der Befehls- und Sicherheitsaktualisierungen an verschiedene IPS-Server hervorbringen, die auf einem beliebigen der verschiedenen Knoten des Netzes **200** gemäß einem Ausführungsbeispiel der Erfindung arbeiten. Jeder Server oder Knoten **201A–201L**,

202A–202T, 203A–203M, 204A–204U, 205A–205Q, 206A–206V, 207A–207N, 208A–208P, 209A–209W, 210A–210R und 211A–211X ist vorzugsweise mit der allgemeinen Beschreibung des Knotens **270**, der vorstehend beschrieben ist, konform, und jeder Knoten betreibt vorzugsweise eine Instanz der IPS-Vorrichtung **91** und unterhält eine jeweilige Datenbank **277** von Signaturdateien, die durch den jeweiligen Knoten gefiltert werden können. Der Inhalt der Instanz der Datenbank **277** kann sich von Knoten zu Knoten unterscheiden, und die maschinenlesbaren Signaturen, die in demselben gespeichert sind, können periodisch modifiziert, gelöscht oder erweitert werden.

[0042] Gemäß einem Reduzieren der erforderlichen Bandbreitenkapazität des IPS-Verwaltungsknoten **85** können die Knoten, die eine IPS-Vorrichtung **91** betreiben, logische Gruppenbezeichnungen aufweisen, die denselben zugeordnet sind, auf die gemeinsame Sicherheitsvorschriften angewendet werden können. Zum Beispiel können die Mailserver 210A–211X einander logisch zugeordnet sein, weil sie, aufgrund der Gemeinsamkeit ihrer Dienste, durch identische Angriffe ins Ziel gefaßt werden können, die keine anderen Knoten beeinträchtigen, die andere Netzdienste liefern. So wird eine Sicherheitsaktualisierung, wie Signaturdateien, die maschinenlesbare Angriffssignaturen aufweisen, die auf einen SMTP-Angriff (SMTP = simple mail transfer protocol = einfaches Mail-Übertragungsprotokoll) bezogen sind, die durch das Netz ausgestrahlt wird, durch alle Knoten empfangen, die eine IPS-Instanz aufweisen, die auf denselben ungeachtet der Tatsache, ob der zugeordnete Knoten für einen solchen Angriff anfällig ist oder nicht, installiert ist. Neben dem Erfordernis einer Verarbeitungs- und Übertragungsbandbreite, die im wesentlichen am Verwaltungsknoten **85** verschwendet wird, der zum Erzeugen und Übertragen der Sicherheitsaktualisierung verantwortlich ist, kann eine Netzbandbreite in ineffizienter Weise zum Ausstrahlen der Aktualisierungsnachricht an die Knoten verwendet werden, die keinen Schutz vor der Sicherheitsmaßnahme, die durch die ausgestrahlte Nachricht geliefert wird, erfordern. Zusätzlich installieren übliche IPS all diese Sicherheitsaktualisierungen und setzen die Verarbeitung der Signaturen fort, die somit jedesmal geliefert werden, wenn ein Rahmen oder ein Paket durch das IPS analysiert wird. Im Laufe der Zeit kann ein gegebener Knoten zahlreiche Sicherheitsaktualisierungen zusammentragen, die Sicherheitsmaßnahmen liefern, die den Angriffen zugeordnet sind, die auf den Knoten nicht zutreffen. Die Verarbeitung solcher Sicherheitsmaßnahmen ist ineffizient und kann zu Betriebsverlusten und Ineffizienzen der IPS-Vorrichtung **91** sowie zu Betriebsverlusten des hostenden Knotens führen.

[0043] Unter Bezugnahme auf **Fig. 7** ist eine logische Gruppierung von Knoten dargestellt, die im Netz **200** angeordnet ist, die eine Gruppensendung von Befehls- und Sicherheitsaktualisierungen vom Verwaltungsknoten **85** gemäß einem Ausführungsbeispiel der vorliegenden Erfindung erleichtert. Die Webserver 201A–202T können durch einen Verwaltungsknoten **85** basierend auf der Gemeinsamkeit der Dienste, die jeweils durch denselben bereitgestellt werden, logisch zugeordnet sein. Folglich kann eine Identifizierung der Logische-Zuordnungsgruppierungs-Webserver 201A–201T zugeordnet und unter den Webservern 201A–201T aufgeteilt werden, so daß die Befehls- und Sicherheitsaktualisierungen, wie Angriffssignaturen, die Signaturen von Angriffen definieren, die an einen Webinhalts-Server gerichtet werden können, im allgemeinen adressiert und nur an jene Knoten verteilt werden können, die dadurch eventuell betroffen sind, d. h. die Identifizierung der logischen Zuordnung dient dazu, einen oder mehrere Knoten des Netzes **200** in logische Gruppen zu gruppieren, wobei jeder Knoten in einer Gruppe im allgemeinen für eine spezielle Ausbeutung anfällig ist. Bei einem exemplarischen Ausführungsbeispiel ist die Identifizierung vorzugsweise als ein IP-Gruppensenden-Gruppen-ID implementiert. Folglich ist der Gruppensenden-Gruppen-ID A vorzugsweise eine 28-Bit-Gruppensenden-Identifizierung, und die Server 201A–202T weisen so eine Host-Gruppe **215** auf. Andere Server können der Host-Gruppe **215** hinzugefügt werden, die aus Webservern 201A–202T besteht, und die Server, die in der Host-Gruppe **215** umfaßt sind, können aus derselben durch hinreichend bekannte Mechanismen wie IGMP-Berichte (IGMP = Internet group management protocol = Internetgruppenverwaltungsprotokoll) entfernt werden. Andere Gruppensenden-Mechanismen, wie UDP-Gruppensenden-Mechanismen (UDP = user datagram protocol = Benutzerdatagrammprotokoll) können an deren Stelle eingesetzt werden. Um das Gruppensenden über separate Netze 200A–200N zu realisieren, sind die Router 160A–106M vorzugsweise gruppensendefähig, so daß die Gruppensenden-Nachrichten Adressen aufweisen können, die über den verschiedenen Netzen 200A–200N, die Hosts aufweisen, die den gemeinsamen Gruppensenden-Gruppen angehören, aufgelöst werden können.

[0044] In ähnlicher Weise können die FTP-Server 203A–204U logisch zugeordnet sein und eine FTP-Hostgruppe **216** aufweisen und eine Gruppensenden-Gruppen-ID B aufweisen, der denselben durch den Verwaltungsknoten **85** zugeordnet wird. Desgleichen können die Dateiserver 205A–206V eine Gruppensenden-Gruppen-ID C, die denselben zugeordnet ist, aufweisen und eine Dateiserver-Hostgruppe **217** aufweisen, die Datenbankserver 207A–207W können einen Gruppensenden-Gruppen-ID D, der denselben zugeordnet ist, aufweisen und eine Datenbankserver-Rostgruppe **218** aufweisen, und die Mailserver 210A–211X können einen Gruppensenden-Gruppen-ID Z, der denselben zugeordnet ist, aufweisen und eine Mailserver-Hostgruppe **219** aufweisen.

[0045] Folglich kann der Verwaltungsknoten **85** Befehls- und Sicherheitsaktualisierungen an die Server von einer oder mehreren Rostgruppen über eine Gruppensendung synchronisieren. Das erforderliche Betriebsmittel und die Bandbreite des Verwaltungsknotens **85** wird so reduziert. Vorzugsweise werden die Befehls- und Sicherheitsaktualisierungen, die über eine Gruppensenden-Nachricht geliefert werden, zwischen dem Verwaltungsknoten **85** und der adressierten Gruppensenden-Gruppe verschlüsselt. So kann die Datenintegrität durch Validieren der Netzrahmenanfangsblöcke gegenüber einem Integritätsalgorithmus, der an jedem Knoten ausgeführt wird, der in einer Hostgruppe umfaßt ist, beibehalten werden. Die Kommunikationsauthentifizierung kann durch Einrichtung und Authentifizieren einer Sitzung ausgeführt werden, die zum Ausführen der Aktualisierungen verwendet wird. Die Sicherheitsaktualisierungen, die durch einen Knoten des Netzes **200** gemäß der vorstehend beschriebenen Verteilungstechnik empfangen werden, können dann in der Datenbank **277** gespeichert und einer beispielhaften assoziativen Prozeßmaschine zugeführt werden, die zum Filtern von Netzpaketen und/oder Rahmen dureh die mitanhängige Anmeldung mit dem Titel "Method, Node and Computer Readable Medium for Identifying Data in an Network Exploit" beschrieben und hiermit gleichzeitig eingereicht wird.

[0046] Es wird darauf hingewiesen, daß die Miteinbeziehung eines Knotens in eine Hostgruppe **215–219** nicht die Einbeziehung des Knotens innerhalb einer anderen Hostgruppe ausschließt, sondern vielmehr kann ein gegebener Knoten innerhalb mehrerer Hostgruppen **215–219** umfaßt sein. Zusätzlich können die netzbasierten IPS-Vorrichtun-

gen **180–182** innerhalb einer oder mehrerer Hostgruppen **215–219** umfaßt sein.

Patentansprüehe

1. Netz (**200**) mit einem Einbruchschutzsystem, das folgende Merkmale aufweist:
ein Netzmedium (**200B**);
einen Verwaltungsknoten (**85**), der mit dem Netzmedium (**200B**) verbunden ist und eine Einbruchpräventionssystem-Verwaltungsanwendung (**279**) betreibt; und eine Mehrzahl von Knoten (**215–219**), die mit dem Netzmedium (**200B**) verbunden ist und ein Exemplar einer Einbruchschutzsystem-Anwendung (**91**) betreiben, wobei zumindest einer der Knoten eine Identifizierung aufweist, die demselben zugeordnet ist, basierend auf einer logischen Zuordnung, die einen oder mehrere der Mehrzahl von Knoten (**215–219**) gruppiert, wobei alle Knoten, die eine Identifizierung gemeinsam verwenden, gemeinsam für zumindest eine Netzausbeutung anfällig sind.

2. Netz (**200**) gemäß Anspruch 1, bei dem der Verwaltungsknoten (**85**) betreibbar ist, um eine Sicherheitsaktualisierung zu verursachen, die an jeden Knoten übertragen wird, der die Identifizierung gemeinsam verwendet, wobei beliebige verbleibende Knoten, die die Identifizierung nicht gemeinsam verwenden, von einem Empfangen der Aktualisierung ausgeschlossen sind.

3. Netz (**200**) gemäß Anspruch 1 oder 2, bei dem eine Mehrzahl von Identifizierungen jeweils einem oder mehreren der Mehrzahl von Knoten (**215–219**) zugeordnet ist.

4. Netz (**200**) gemäß einem der Ansprüche 1 bis 3, das ferner folgende Merkmale aufweist:
eine Mehrzahl von Netzmedien (**200A–200N**); und
zumindest einen Router (**160A–160M**), wobei jeder des Verwaltungsknotens (**85**) und der Mehrzahl von Knoten (**215–219**) jeweils einem der Mehrzahl von Netzmedien (**200A–200N**) im Netz (**200**) zugeordnet ist, wobei der Router (**160A–160M**) zwischen der Mehrzahl von Netzmedien (**200A–200N**) angeordnet ist und betreibbar ist, um die Sicherheitsaktualisierung von dem Netzmedium (**200B**), mit dem der Verwaltungsknoten (**85**) verbunden ist, an alle Knoten weiterzuleiten, die mit den verbleibenden Netzmedien (**200A, 200C–200N**) verbunden sind und die Identifizierung gemeinsam verwenden.

5. Netz (**200**) gemäß Anspruch 4, bei dem der Router (**160A–160M**) bestimmt, ob ein beliebiger der Mehrzahl von Knoten (**215–219**), die mit den verbleibenden Netzmedien verbunden sind, die Identifizierung durch die Implementierung des Internet-Gruppenverwaltungsprotokolls gemeinsam verwendet.

6. Verfahren zum Übertragen einer Aktualisierungsnachricht an einen Teilsatz von Knoten (**215–219**) einer Mehrzahl von Netzknoten, wobei das Verfahren folgende Schritte aufweist:
Erzeugen der Aktualisierungsnachricht durch einen Verwaltungsknoten (**85**) des Netzes (**200**);
Adressieren der Aktualisierungsnachricht an eine Netzadresse, die durch den Teilsatz von Knoten (**215–219**) des Netzes (**200**) gemeinsam verwendet wird;
Übertragen der Aktualisierungsnachricht; und
Empfangen und Verarbeiten der Aktualisierungsnachricht durch den Teilsatz von Knoten (**215–219**).

7. Verfahren gemäß Anspruch 6, bei dem ein Adressieren der Aktualisierungsnachrieht an eine Netzadresse, die durch den Teilsatz von Knoten (**215–219**) gemeinsam verwendet wird, ferner ein Adressieren der Aktualisierungsnachrieht an eine Internetprotokoll-Gruppensenden-Gruppenidentifizierung aufweist, wobei der Teilsatz von Knoten (**215–219**) einer Hostgruppe angehört, die der Gruppensenden-Gruppenidentifizierung zugeordnet ist.

8. Verfahren gemäß Anspruch 6 oder 7, bei dem das Übertragen der Aktualisierungsnachricht durch das Netz (**200**) ferner folgende Schritte aufweist:
Übertragen der Aktualisierungsnachricht auf einem Netzmedium (**200B**), auf dem der Verwaltungsknoten (**85**) verbunden ist;
Empfangen der Aktualisierungsnachricht durch einen Router (**160A–160M**), der das Netzmedium (**200B**), auf dem der Verwaltungsknoten (**85**) verbunden ist, abschließt; und
Weiterleiten, durch den Router (**160A, 160C**), der Aktualisierungsnachricht an alle Knoten, die in dem Teilsatz von Knoten (**215–219**) auf einem zweiten Netzmedium (**200A, 200C–200N**), das durch den Router (**160A–160M**) geschlossen ist, umfaßt sind.

9. Verfahren gemäß einem der Ansprüche 6 bis 8, bei dem das Übertragen der Aktualisierungsnachricht an einen Teilsatz von Knoten (**215–219**) ferner ein Übertragen der Aktualisierungsnachricht an entweder zumindest einen Einbruchschutzsystemknoten oder eine netzbasierte Einbruchschutzsystemvorrichtung (**180–182**) aufweist.

10. Computerlesbares Medium, auf dem ein Satz von Instruktionen gespeichert ist, die ausgeführt werden sollen, wobei der Satz von Instruktionen, wenn dieselben durch einen Prozessor (**272**) ausgeführt werden, bewirkt, daß der Prozessor (**272**) ein Computerverfahren ausführt, das folgende Schritte aufweist:
Erzeugen, durch den Computer, einer Nachricht, die an einen Teilsatz von Knoten (**215–219**) auf einem Netz (**200**) adressiert ist;
Übertragen der Nachricht auf einem Netzmedium (**200B**) des Netzes (**200**) an den Teilsatz von Knoten (**215–219**); Empfangen der Nachricht durch einen Router (**160A–160M**), der das Netzmedium abschließt; und
Weiterleiten, durch den Router, der Nachricht an alle Knoten, die in dem Teilsatz von Knoten (**215–219**) auf einem zweiten Netzmedium (**200A, 200C–200M**) umfaßt sind, das durch den Router (**160A–160M**) abgeschlossen ist.

Hierzu 6 Seite(n) Zeichnungen

- Leerseite -

Nummer: DE 102 49 842 A1
Int. Cl.[7]: H04L 12/26
Offenlegungstag: 28. Mai 2003

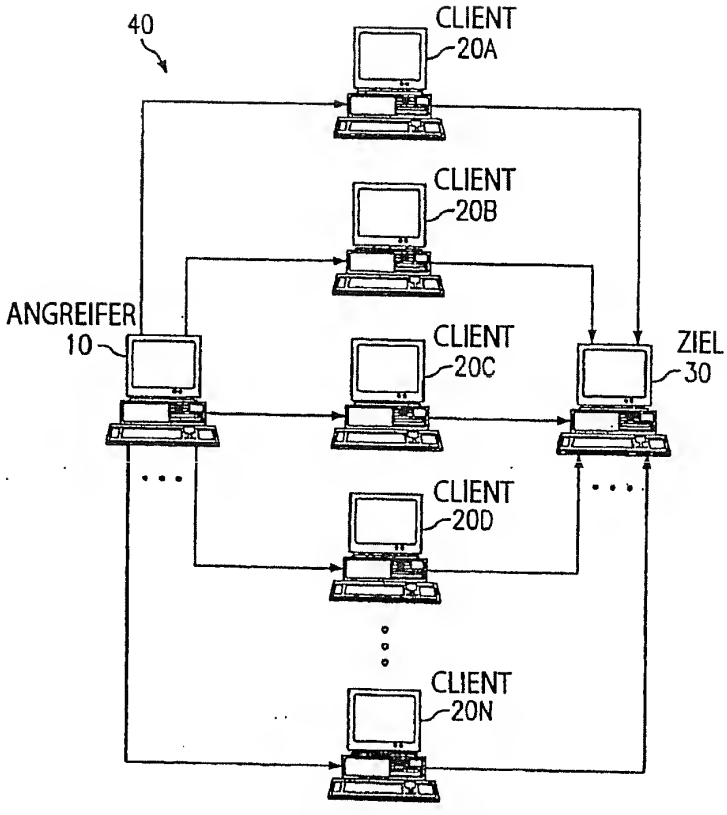
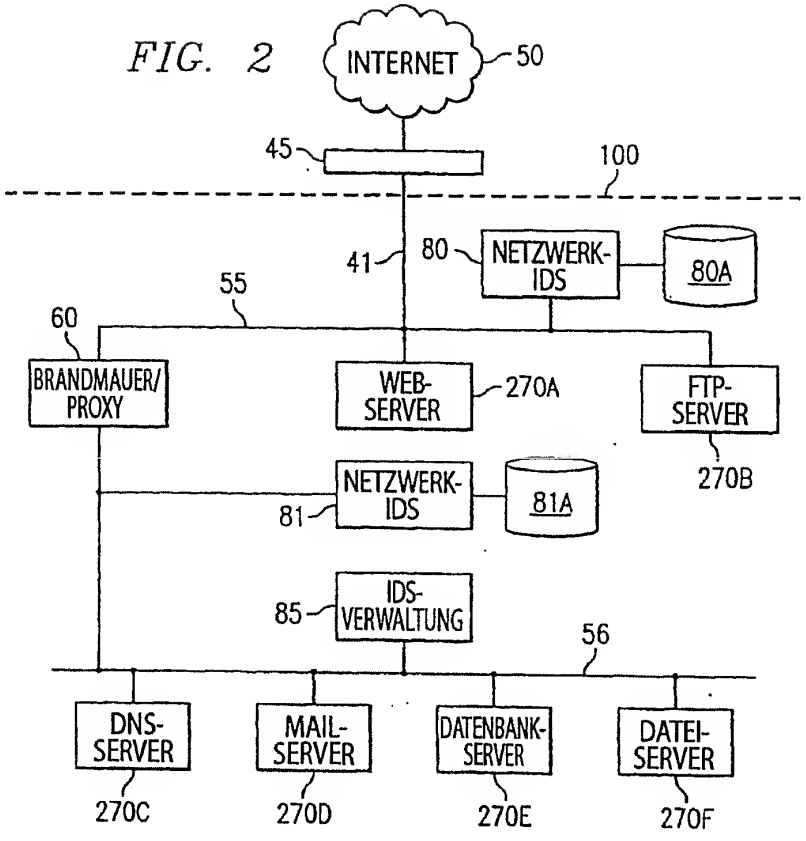


FIG. 1

Nummer: DE 102 49 842 A1
Int. Cl.[7]: H 04 L 12/26
Offenlegungstag: 28. Mai 2003

FIG. 2



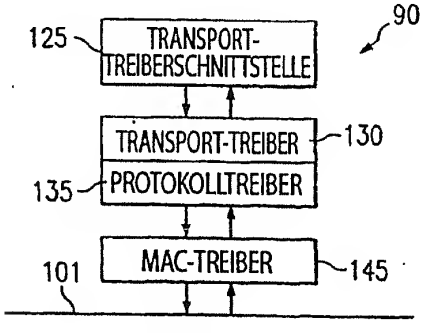
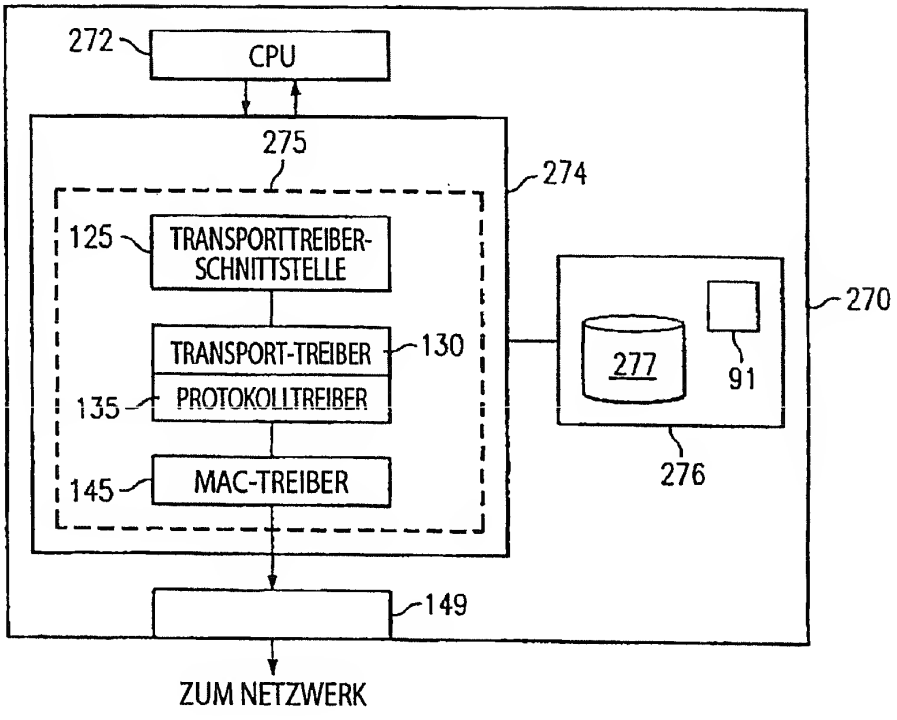


FIG. 3

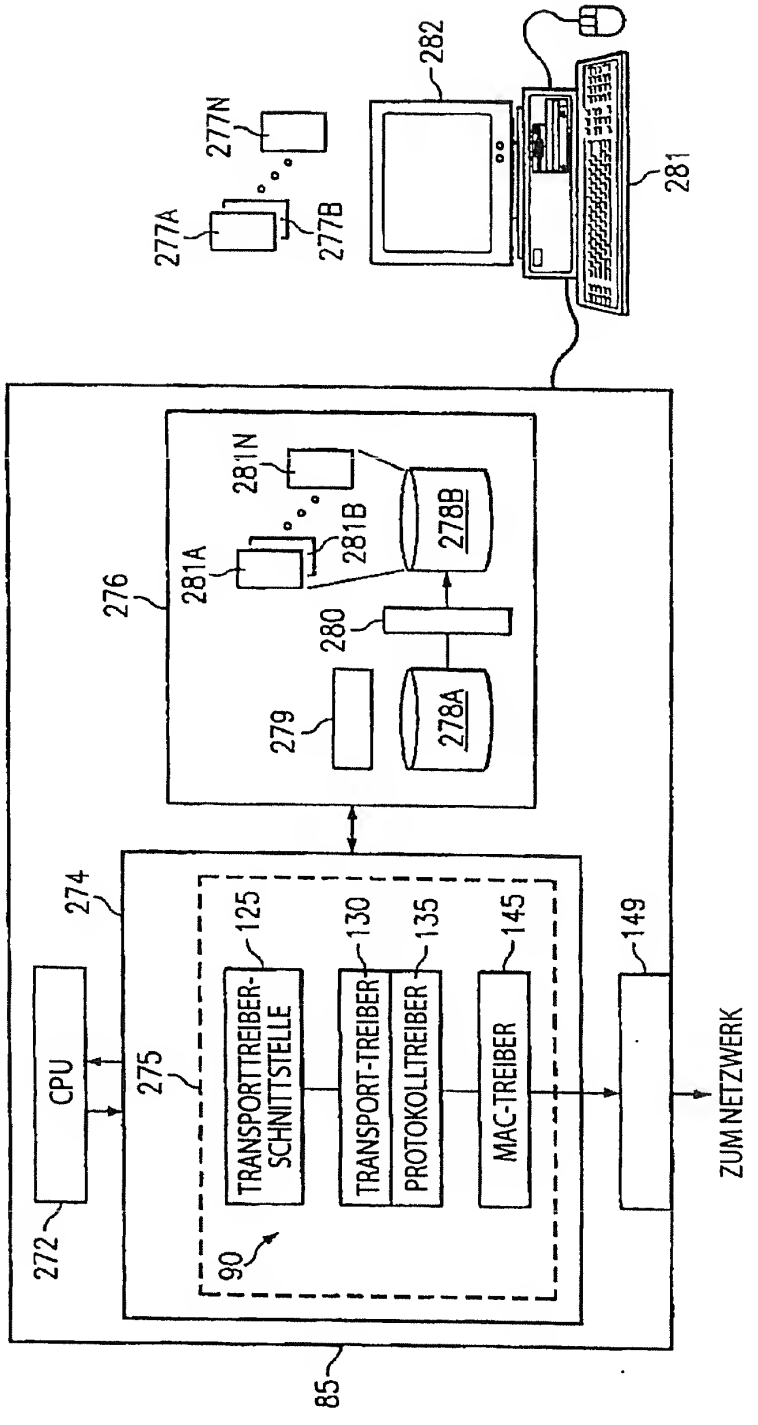
Nummer: DE 102 49 842 A1
Int. Cl.[7]: H 04 L 12/26
Offenlegungstag: 28. Mai 2003

FIG. 4



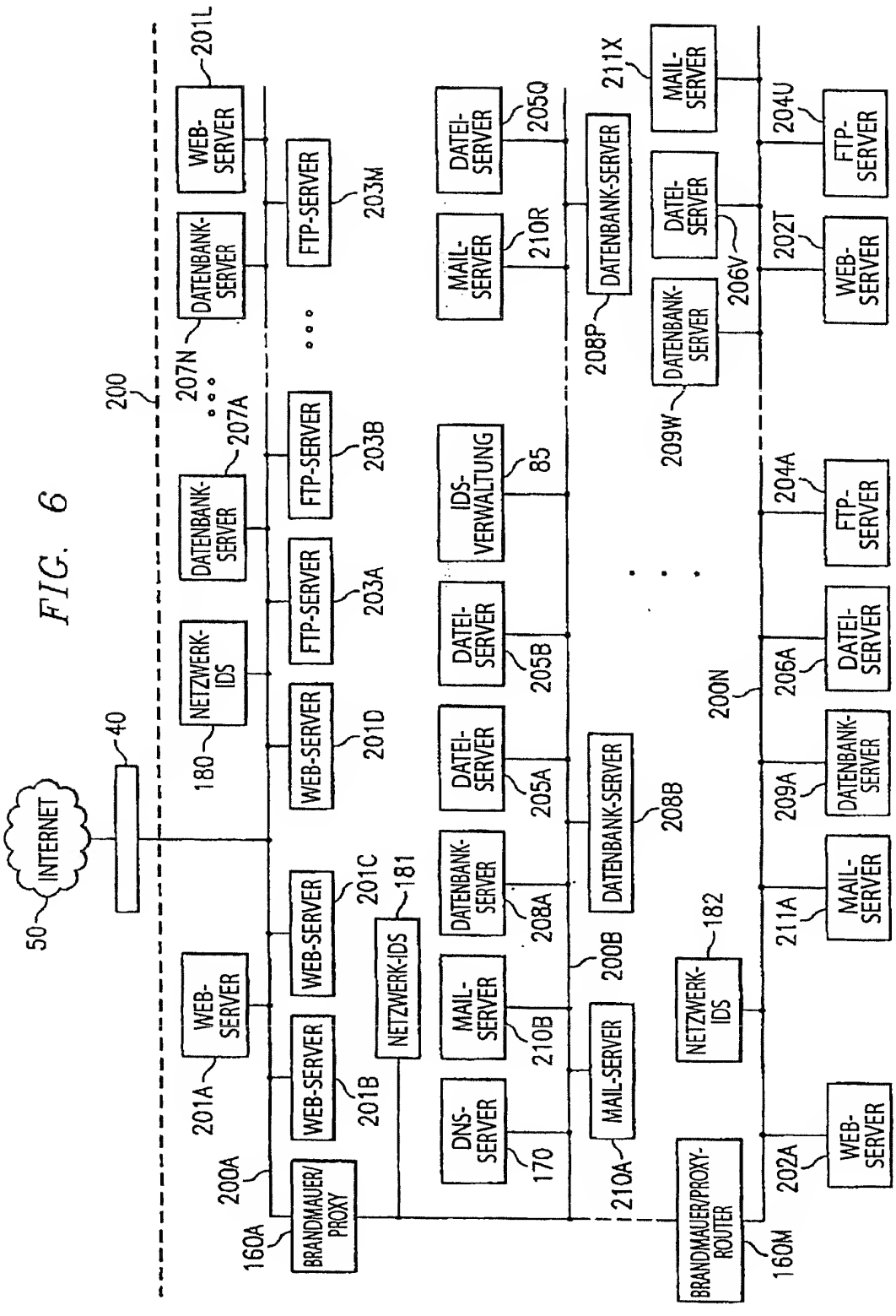
Nummer: DE 102 49 842 A1
Int. Cl.[7]: H 04 L 12/26
Offenlegungstag: 28. Mai 2003

FIG. 5



Nummer: DE 102 49 842 A1
Int. Cl.[7]: H 04 L 12/26
Offenlegungstag: 28. Mai 2003

FIG. 6



Nummer: DE 102 49 842 A1
Int. Cl.[7]: H04L 12/26
Offenlegungstag: 28. Mai 2003

FIG. 7